UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS

DAVID HOUSE,)	
Plaintiff,)	
v.)	
)	Case No. 1:11-cv-10852-DJC
JANET NAPOLITANO, in her official capacity as)	
Secretary of the U.S. Department of Homeland)	
Security; ALAN BERSIN, in his official capacity as)	
Commissioner, U.S. Customs and Border Protection;)	
JOHN T. MORTON, in his official capacity as Director,)	
U.S. Immigration and Customs Enforcement,)	
)	
Defendants.)	
)	

DEFENDANTS' MEMORANDUM IN SUPPORT OF THEIR MOTION TO DISMISS, OR IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

		<u>PAGE</u>
LEGA	AL BAC	KGROUND
I.	The G	overnment's Authority to Conduct Border Searches
	A.	Searches and Inspections of Electronic Devices
	B.	Seeking Assistance to Search Electronic Devices
FACT	AL BA	CKGROUND6
I.	PLAIN	NTIFF'S ALLEGATIONS
II.	PLAIN	TIFF'S CLAIMS AND PRAYER FOR RELIEF
ARGU	JMENT	
I.	STAN	DARD OF REVIEW 8
II.	PLAIN	NTIFF'S FOURTH AMENDMENT CLAIM SHOULD BE DISMISSED9
	A.	The Search and Detention of Plaintiff's Devices Occurred at the Border9
	В.	The Government Needs Neither a Warrant nor Reasonable Suspicion When Searching Closed Containers, Such as Electronic Devices, at the Border Because Such Searches are Not Personally Invasive, and are not Conducted in a Particularly Offensive or Destructive Manner
	C.	Electronic Devices Are Closed Containers, and, as Such, Can Be Searched and Inspected at the Border Without Individualized Suspicion
	D.	Plaintiffs' Allegations that he was Targeted for the November 3, 2010 Search and Detention of his Electronic Devices Fail to State a Claim For Relief Under the Fourth Amendment
	E.	Detaining Devices is Consistent With the Government's Need to Adequately Inspect The Items Before They Enter the United States

	F.	In the Alternative, Even if the Court Finds that Plaintiff has Stated a Claim for a Fourth Amendment Violation, the Undisputed Material Facts Show that the Detention of Plaintiff's Devices was Reasonable, and the Court Should Award Summary Judgment to the Government on this Claim	. 22
III.	PLAIN	TIFF'S FIRST AMENDMENT CLAIMS SHOULD BE DISMISSED	23
	A.	The November 3, 2010 Search and Inspection of Plaintiff's Devices Did not Violate his First Amendment Rights	24
	B.	Plaintiff's Associational Privacy Claim Should Be Dismissed	25
CONC	LUSIO	N	29

TABLE OF AUTHORITIES

CASES	PAGE(S)
Almeida-Sanchez v. United States, 413 U.S. 266 (1973)	9
Ashcroft v. Iqbal, 556 U.S, 129 S. Ct. 1937 (2009)	passim
Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007)	8
Bond v. United States, 529 U.S. 334 (2000)	18
Brown v. Socialist Workers '74 Campaign Comm. (Ohio), 459 U.S. 87 (1982)	28
Cancel-Rios v. United States, No. 10-1386, 2010 WL 3420805 (D.P.R. Aug. 30, 2010)	13
Church of Scientology of Cal. v. Simon, 460 F. Supp. 56 (C.D. Cal. 1978)	14, 24
In re Colonial Mortgage Bankers Corp., 324 F.3d 12 (1st Cir. 2003)	4
Decotiis v. Whittemore, 635 F.3d 22 (1st Cir. 2011)	8
Doyle v. N.Y. State Div. of Hous. and Comm'ty Renewal, No. 98- 2161, 1999 WL 177441 (S.D.N.Y. Mar. 30, 1999)	27
Illinois v. Caballes, 543 U.S. 405 (2005)	23
Lyng v. Int'l Union, 485 U.S. 360 (1988)	25
Maldonado v. Fontanes, 568 F.3d 263 (1st Cir. 2009)	8
Miss. Pub. Empl. Ret. Sys. v. Boston Sci. Corp., 523 F.3d 75 (1st Cir. 2008)	4

Case 1:11-cv-10852-DJC Document 11 Filed 07/28/11 Page 5 of 39

10 Re Motor Fuel Temperature Sales Practices Litig., 641 F.3d 470 (10th Cir. 2011)	25, 27
NAACP v. Alabama, 357 U.S. 449 (1958)	28
Pealbert-Rosa v. Fortuo-Burset, 631 F.3d 592 (1st Cir. 2011)	8
Rahman v. Chertoff, 530 F.3d 622 (7th Cir. 2008)	11
Rivera v. Centro Medico de Turabo, Inc., 575 F.3d 10 (1st Cir. 2009)	9
Roberts v. United States Jaycees, 468 U.S. 609 (1984)	25
Sanchez v. Pereira-Castillo, 590 F.3d 31 (1st Cir. 2009)	8
Scott v. United States, 436 U.S. 128 (1975)	18
Shaw v. Digital Equip. Corp., 82 F.3d 1194 (1st Cir.1996)	4
Tabbaa v. Chertoff, 509 F.3d 89 (2d Cir. 2007)	passim
Untied States v. Borello, 766 F.2d 46 (2d Cir. 1985)	23, 24
United States v. Cotterman, 637 F.3d 1068 (9th Cir. 2011)	passim
United States v. 12 200-Ft. Reels of Super 8mm, 413 U.S. 123 (1973)	14
United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006)	21
United States v. Amaro-Rodriguez, No. 08-378, 2010 WI, 503063 (D.P.R. Feb. 8, 2010)	11

Case 1:11-cv-10852-DJC Document 11 Filed 07/28/11 Page 6 of 39

United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008)
United States v. Barrow, 448 F.3d 37 (1st Cir. 2006)
United States v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008)
United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009)
United States v. Chaudhry, 424 F.3d 1051 (9th Cir. 2005)
United States v. Flores-Montano, 541 U.S. 149 (2004) passim
United States v. Giberson, 527 F.3d 882 (9th Cir. 2008)
United States v. Hampe, No. CR 07-3-B-W, 2007 WL 1192365 (D. Me. Apr. 18, 2007)
United States v. Hill, 459 F.3d 966 (9th Cir. 2006)
United States v. Hill, 322 F. Supp. 2d 1081, 1089 (C.D. Cal. 2004)
United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) passim
United States v. Irving, 452 F.3d 110 (2d Cir. 2006)
United States v. Irving, No. 03-cr-633, 2003 WL 22127913 (S.D.N.Y. Sept. 15, 2003), aff'd, 452 F.3d 110 (2d Cir. 2006)
United States v. Lawson, 461 F.3d 697 (6th Cir. 2006)
United States v. Linarez-Delgado, 259 Fed. Appx. 506 (3d Cir. 2007)

Case 1:11-cv-10852-DJC Document 11 Filed 07/28/11 Page 7 of 39

United States v. McAuley, 563 F. Supp. 2d 672 (W.D. Tx. 2008)	4
United States v. Mitchell, No. CR407-126, 2007 WL 2915889 (S.D. Ga. Oct 3, 2007)	0
United States v. Montoya de Hernandez, 473 U.S. 531 (1985) passir	n
United States v. Pickett, No. 07-374, 2008 WL 4330247 (E.D. La. Sept. 16, 2008), aff'd, 598 F.3d 231 (5th Cir. 2010)	3
United States v. Ramsey, 431 U.S. 606 (1977) passir	n
United States v. Seljan, 547 F.3d 993 (9th Cir. 2008), cert. denied, 129 S. Ct. 1368 (2009) passin	n
United States v. Stabile, 633 F.3d 219 (10th Cir. 2011)	1
United States v. Triumph Capital Group, Inc., 211 F.R.D. 31 (D. Conn. 2002)	0
United States v. Veema, No. H-08-699-1, 2010 WL 1427261 (S.D. Tex. Apr. 8, 2010)	3
United States v. Villamonte-Marquez, 462 U.S. 579 (1983)	8
United States v. Williams, 592 F.3d 511 (4th Cir. 2010)	5
Whren v. United States, 517 U.S. 806 (1996)	8
Washington Legal Found. v. Mass. Bar Found., 993 F.2d 962 (1st 1Cir. 1993)	8
Zurcher v. Stanford Daily, 136 U.S. 547 (1978)	3

STATUTES

6 U.S.C. §§ 111(b)(1)(A) & 202(1)	3
6 U.S.C. § 202(2), (4) & (6)	. 3
8 U.S.C. § 1357	. 4
19 U.S.C. § 482	. 4
19 U.S.C. § 507	22
19 U.S.C. § 1305	. 4
19 U.S.C. § 1496	. 4
19 U.S.C. § 1499	. 4
19 U.S.C. § 1581	. 4
19 U.S.C. § 1582	. 4
19 U.S.C. § 1583	. 4
19 U.S.C. § 1589a	. 4
31 U.S.C. § 5317	. 4
42 U.S.C. § 2000aa(a)	23
42 U.S.C. § 2000aa-5	23
Act of July 31 1789 ch 5 1 Stat 29	4

RULES AND REGULATIONS

15 C.F.R. § 758.7
19 C.F.R. § 148.21
19 C.F.R. § 162.6
19 C.F.R. § 162.7
RULES OF CIVIL AND CRIMINAL PROCEDURE
Fed. R. Civ. P. 12(b)(6)
Fed. R. Civ. P. 56(a) passin

The Government's authority to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive. This long-standing authority extends to suitcases, trunks, and handbags, as well as electronic devices. Plaintiff's complaint requests a new exception for electronic devices from the Government's authority to conduct routine searches of closed containers at the border. This, Plaintiff claims, is necessary because of the personal and confidential nature of materials included on electronic devices. Most courts—including every federal appellate court—which have been faced with such an assertion have rejected this precise claim, concluding that electronic devices are no different from other closed containers, such as luggage or personal effects, and are thus subject to routine, suspicionless border searches. Indeed, courts have long understood that travelers have a greatly diminished expectation of privacy at the international border, and they must expect some intrusion or delay so that the Government may protect itself and its citizens by stopping and examining persons and property crossing into or from this country. Those expectations are no different whether the items involved are luggage and personal effects, vehicles, or electronic devices. Pursuant to this authority, the Government may detain property at the border, and continue to detain that property for the purpose of a border search, even after the individual owner has been processed and has left a port of entry.

Based on this settled law, the specific information contained in Plaintiff's devices is not relevant to the only issue before this Court—namely, did the Government have the authority to conduct a border search of any and all items Plaintiff sought to bring into the United States? The answer to such question is yes. "Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). While Plaintiff

also contends that the Government retained his devices for too long after his re-entry into the United States on November 3, 2010, there is no *per* se rule limiting the amount of time that the Government may expend in pursuit of a lawful border search. To the contrary, courts have permitted the Government the time needed to adequately conduct a meaningful search. *See United States v. Cotterman*, 637 F.3d 1068, 1083 (9th Cir. 2011). To the extent the Court concludes that Plaintiff has asserted a viable Fourth Amendment claim based on how long his devices were detained, the undisputed material facts (as reflected in Defendants' Rule 56.1 statement) establish that the Government's detention of Plaintiff's devices was reasonable.

Plaintiffs' claims should therefore be dismissed on the merits pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. There is no basis for the Court to conclude that searches of laptops or other electronic devices at the border should be subjected to a different standard than that for other closed containers. Nor is there a basis for the Court to conclude that Plaintiff's First Amendment rights were violated simply because Plaintiff believed the information contained on his electronic devices was "private" and allegedly "privileged." Finally, Plaintiff's "associational privacy" claim should also be dismissed, since the Government is not prohibited from examining any items at the border simply because they may be related to the work of an organization or the owner may identify himself as a member of an organization. There are no allegations that show an infringement on Plaintiff's right to association. In the alternative, Defendants seek summary judgment, because the undisputed facts show that the search and inspection of Plaintiff's electronic devices was lawful and appropriate. ¹

¹ Defendants Memorandum is thirty (30) pages in length, in accordance with Court's minute order of July 6, 2011 which granted the parties' joint motion requesting, among other items, permission to file overlength briefs. *See* Dkt. # 8, Parties' Joint Motion, filed July 5, 2011.

LEGAL BACKGROUND

I. THE GOVERNMENT'S AUTHORITY TO CONDUCT BORDER SEARCHES

"[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, we have stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

Defendants in this action include Janet Napolitano, Secretary of the U.S. Department of Homeland Security; Alan Bersin, Commissioner, U.S. Customs and Border Protection; and John T. Morton, Director, U.S. Immigration and Customs Enforcement. The U.S. Department of Homeland Security ("DHS"), through its components U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE"), is the first line of defense at the border, responsible for administering the customs and immigration laws of the United States, securing the borders, and inspecting individuals and items that seek entry into and propose exit from the United States. *See* 6 U.S.C. § 202(2), (4) & (6).

One of DHS' most important responsibilities is "preventing the entry of terrorists and the instruments of terrorism into the United States." 6 U.S.C. §§ 111(b)(1)(A) & 202(1). DHS is also responsible for enforcing hundreds of laws and regulations, including, among others, those addressing immigration, currency and financial transactions, customs, commerce and trade, copyrights and trademarks, narcotics, the safety of agricultural products and other goods, and

import and export controls on wildlife and plants, chemical and biological weapons, guns, and other items.² In light of these numerous, varied, and important responsibilities, customs officers have exercised broad authority to inspect travelers and their baggage as they cross the international border for more than two centuries.³

A. Searches and Inspections of Electronic Devices

In August 2009, CBP and ICE issued policies on their longstanding authority to search and inspect electronic devices at the border. *See* Defendants L.R. 56.1 Statement, ("Defs. 56.1 St.). ¶ 19 (citing ICE Directive No 7-6.1, as well as CBP Directive No. 3340-049). The policies relate exclusively to border searches of electronic devices—that is, searches of travelers' electronic devices performed at the international border, or its functional equivalent, by properly authorized CBP officers or ICE agents (hereinafter "customs officers"). *See* ICE Directive ¶¶ 1.1, 8.1(1); *see also* CBP Directive, ¶ 1. Border searches of electronic devices are "a crucial tool for detecting information [relating to] terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws." ICE Directive ¶ 4; *see also* CBP Directive,

_

² See generally Summary of Laws and Regulations Enforced by CBP (2005), http://www.cbp.gov/xp/cgov/trade/legal/summary laws enforced/: these same laws and regulations are investigated and prosecuted by ICE.

³ See Act of July 31, 1789, ch. 5, 1 Stat. 29; see also, e.g., 19 U.S.C. §§ 482 (authority to search vehicles and persons), 1461 (authority to search "[a]ll merchandise and baggage" brought into the United States), 1496 (authority to search baggage of persons entering the United States), 1499(a) (authority to examine and detain imported merchandise), 1305 (authority to search for potentially obscene material), 1581 (authority to board vessels and search), 1582 (authority to detain and search "all persons coming into the United States from foreign countries"), 1583 (authority to examine outbound mail), 1589a (general law enforcement authority), 1595a(c)(3) (authority to detain merchandise introduced contrary to law); 8 U.S.C. § 1357 (authority of immigration officers to board and search); 31 U.S.C. § 5317 (authority regarding search and forfeiture of monetary instruments); 15 C.F.R. § 758.7; 19 C.F.R. §§ 162.6 and 162.7.

⁴ Copies of the ICE and CBP Directives are attached to Defendants' Rule 56.1 statement. *See* Defs. 56.1 St., ¶ 19 & Exs. 5-6. The Directives are incorporated by reference into the Complaint. *See* Compl. ¶¶ 24-26. Defendants' Memorandum primarily discusses the ICE policy since ICE was the agency involved in the detention of Plaintiff's devices. *See* Defs. L.R. 56.1 St. ¶¶ 2-6 (citing to declarations).

¶ 1. As described below, these policies have been carefully crafted to provide the Government, through DHS and its components, with the tools necessary to secure the nation's border, while striving to protect personal privacy to the greatest extent possible.

The policies permit customs officers to search, analyze, and review information contained in electronic devices "with or without individualized suspicion," subject to the guidelines set forth in the policy directives and any other applicable laws. *See* ICE Directive ¶ 6.1; *see also* CBP Directive ¶ 5. The policies recognize that it is not always possible to complete the search of a traveler's electronic device while he or she waits at the border. ICE Directive ¶ 6.1; *see also* CBP Directive ¶ 5.3.1. ICE policy requires its agents "to complete the search of [a] detained electronic device[], or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search." ICE Directive ¶ 8.3(1). The ICE Directive provides that such searches are generally to be completed within thirty calendar days of the date of the detention, unless circumstances exist that warrant more time and appropriate authorization is obtained. *Id*.

B. Seeking Assistance to Search Electronic Devices

Recognizing that customs officers may encounter technical difficulties, encrypted information, or information in a foreign language that would preclude a meaningful and effective search of an electronic device, the policies permit customs officers to seek translation, encryption, and/or other technical assistance, without individualized suspicion. *See* ICE Directive ¶ 8.4(1); CBP Directive ¶¶ 5.3.2.2., 5.3.2.3. Customs officers may also seek subject matter assistance from other federal agencies — i.e., assistance with the "meaning, context, or value of information" contained on the electronic device — if the officers possess reasonable

suspicion of activities in violation of laws enforced by DHS. See ICE Directive \P 8.4(2); see also CBP Directive $\P\P$ 5.3.2.2., 5.3.2.3.

Once the border search of an electronic device is complete, the policies permit customs officers to seize and retain an electronic device, or copies of the information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is "probable cause of unlawful activity." ICE Directive, ¶ 8.5(1)(a); see also CBP Directive ¶ 5.4.1.1. Except as otherwise provided, if customs officers determine that probable cause for a seizure does not exist, any detained electronic device will be returned to the traveler, and any copies of the information contained therein — including any sensitive or privileged information — will be destroyed. See ICE Directive ¶¶ 8.1(5), 8.5(1)(e), 8.5(2)(b); see also CBP Directive ¶ 5.4.1.6.

FACTAL BACKGROUND

I. PLAINTIFF'S ALLEGATIONS

Plaintiff's claims center on his return to the United States on November 3, 2010 from a vacation in Mexico, on a flight from Mexico to Chicago's O'Hare International Airport. Compl. ¶¶ 15-23. As part of his return to the United States, Plaintiff proceeded to passport control and a customs inspection by a CBP officer; immediately following the CBP inspection, Plaintiff was questioned by two ICE agents. *Id.* ¶ 16. The ICE agents detained Plaintiff's laptop computer, his USB storage device, his video camera, and his cellular phone. *Id.* ¶¶ 15, 17. Plaintiff contends he was then questioned by the ICE agents, and at the conclusion of this questioning, Plaintiff's cell phone was returned to him; ICE detained the remaining items, and Plaintiff was given a receipt. *Id.* ¶¶ 19-20. Plaintiff alleges he was told his items would be returned via Federal Express within a week. *Id.* Plaintiff's devices were returned to him on December 22,

2010; the package indicated they were sent from a DHS office in New York, although the items had been detained from Plaintiff in Chicago. *Id.* ¶ 22. Plaintiff asserts, on information and belief, that the Government's interest in his electronic devices stems from his involvement with and activity on behalf of the Bradley Manning Support Network, a group of "individuals and organizations" aimed at supporting Bradley Manning, a "U.S. serviceman . . . arrested on suspicion of having disclosed restricted material to the organization WikiLeaks." *Id.* ¶¶ 9, 12.

II. PLAINTIFF'S CLAIMS AND PRAYER FOR RELIEF

Plaintiffs' complaint sets forth three claims. In his first cause of action, Plaintiff alleges that the November 3, 2010 search and detention of his electronic devices (for which he contends he was targeted as a result of his association with the Support Network), as well as the Government's "continued retention and dissemination of the information [the devices] contained, are unreasonable and violate the Fourth Amendment " Compl. ¶ 36. Plaintiff likewise contends that the same actions violated his First Amendment rights. *Id.* ¶ 37. Finally, Plaintiff contends that the "interception and, more particularly, the retention and dissemination of information in Plaintiff's computer and other electronic devices regarding the organization, work, and supporters and donors of the Bradley Manning Support Network violate the right of associational privacy guaranteed by the First Amendment " *Id.* ¶ 38. Plaintiff seeks a declaration that the November 3, 2010 search and detention of his electronic devices was unconstitutional and an order (i) directing Defendants to return or destroy any information unlawfully obtained from him; and (ii) informing him whether and to whom any of his information was disclosed. *See id.* Prayer for Relief ¶¶ A-C.

ARGUMENT

I. STANDARD OF REVIEW

To survive a motion to dismiss, a complaint must allege a plausible set of facts sufficient "to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "This plausibility standard 'asks for more than a sheer possibility that a defendant has acted unlawfully.' Applying the plausibility standard is 'a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Decotiis v. Whittemore*, 635 F.3d 22 (1st Cir. 2011) (quoting *Ashcroft v. Iqbal*, 556 U.S. _____, 129 S. Ct. 1937, 1948-49 (2009)). The Court accepts all "well-pleaded" facts as true and draws reasonable inferences in favor of Plaintiff. *Washington Legal Found. v. Massachusetts Bar Found.*, 993 F.2d 962, 971 (1st Cir. 1993). Complaints that rest on "bald assertions" and "unsupportable conclusions" should be dismissed. *See Peñalbert-Rosa v. Fortuño-Burset*, 631 F.3d 592, 596 (1st Cir. 2011); *Maldonado v. Fontanes*, 568 F.3d 263, 274 (1st Cir. 2009).

Should the Court determine that Plaintiff has stated a viable claim, Defendants have submitted a Rule 56.1 statement (hereinafter "Defs. 56.1 St.") in support of an alternative motion for summary judgment. *See* Fed. R. Civ. P. 12(d). Rule 56(a) of the Federal Rules of Civil Procedure provides that "[a] party may move for summary judgment, identifying each claim or defense—or the part of each claim or defense—on which summary judgment is sought." Summary judgment shall be granted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." *Id.* A party "may

In assessing a rule 12(b)(6) motion to dismiss, the court may consider, in addition to the complaint itself, documents "that are attached to the complaint and 'documents sufficiently referred to in the complaint," *Giragosian v. Bettencourt*, 614 F.3d 25, 27-28 (1st Cir. 2010) (quoting *Miss. Pub. Empl. Ret. Sys. v. Boston Sci. Corp.*, 523 F.3d 75, 86 (1st Cir. 2008)), without converting the motion to one for summary judgment. *In re Colonial Mortgage Bankers Corp.*, 324 F.3d 12, 19 (1st Cir. 2003) (observing that matters of public record are "fair game" in deciding a Rule 12(b)(6) motion). *See Shaw v. Digital Equip. Corp.*, 82 F.3d 1194, 1220 (1st Cir.1996) (court "may properly consider the relevant entirety of a document integral to or explicitly relied upon in the complaint ... without converting the motion into one for summary judgment").

file a motion for summary judgment at any time [unless a different date is set by court order or local rule] until 30 days after the close of all discovery." Fed. R. Civ. P. 56(b).

II. PLAINTIFF'S FOURTH AMENDMENT CLAIM SHOULD BE DISMISSED

Plaintiff contends that the Government needed reasonable suspicion to search and inspect his electronic devices on November 3, 2010, because they contained personal and sensitive information. This argument has been pressed by other litigants in the federal courts in recent years, to no avail. Whatever Plaintiff chose to store, or not store, on his devices is irrelevant because, in addition to being items that Plaintiff sought to bring into the U.S., electronic devices are simply another kind of closed container capable of containing (or storing) contraband or merchandise, and like luggage, such devices can be searched and inspected by the Government at the border without suspicion. Moreover, to the extent that the Court finds that Plaintiff has stated a viable Fourth Amendment claim, the undisputed facts demonstrate that the search and detention of Plaintiff's electronic devices were lawful and appropriate.

A. The Search and Detention of Plaintiff's Devices Occurred at the Border

Plaintiff alleges that he was told he was "free to leave" by the CBP officer and Plaintiff also states that he had "enter[ed] the terminal and [had] start[ed] to walk toward his connecting domestic flight" by the time he was approached by two ICE officers on November 3, 2010. Compl. ¶ 16. But Plaintiff's Complaint refers specifically to the CBP and ICE policies that relate to the Government's authority to search and detain electronic devices at the border, or the functional equivalent of the border, such as O'Hare Airport. *See* Compl. ¶¶ 24-26. Presumably Plaintiff cited these policies because he concedes that he was in fact located at the border during his interactions with ICE on November 3, 2010 at Chicago's O'Hare Airport. As a result, the

⁶ While Plaintiff was not at a land border, he was at the "border" for Fourth Amendment purposes, as he was entering the United States via a flight that originated outside the country. The federal courts have applied the border

Plaintiff's own complaint confirms that the November 3, 2010 search and detention of his devices occurred at the border.⁷

В. The Government Needs Neither a Warrant nor Reasonable Suspicion When Searching Closed Containers, Such as Electronic Devices, at the Border Because Such Searches are Not Personally Invasive, and are not **Conducted in a Particularly Offensive or Destructive Manner**

The Government's authority to search persons and items at the border is at its "zenith." Flores-Montano, 541 U.S. at 152. As a result, although searches must be reasonable, "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior." Montoya de Hernandez, 473 U.S. at 538. At the border, "the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." Flores-Montano, 541 U.S. at 153. For this reason, it has long been acknowledged that "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *Id.* at 152-53 (quoting Ramsey, 431 U.S. at 616). Accordingly, the Supreme Court has held that "[r]outine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant " Montoya de Hernandez, 473 U.S. at 538; see also United States v. Barrow, 448 F.3d 37, 41 (1st Cir. 2006) (same).

search doctrine to searches occurring at the functional equivalent of the border, which is considered "the first point at which an entrant may practically be detained." Almeida-Sanchez v. United States, 413 U.S. 266, 272-73 (1973) ("For example . . . a search of the passengers and cargo of an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City would clearly be the functional equivalent of a border search."). When Plaintiff's flight landed at O'Hare Airport in Chicago, he was at the "functional equivalent" of the border, and the search and inspection of Plaintiff's electronic devices (as well as any questions that were asked of Plaintiff by either CBP or ICE personnel) were conducted pursuant to the government's border search authority.

⁷ The Government has included citations in its Rule 56.1 Statement to the declarations of CBP Officer Robert Harris and ICE Agents Marcial Santiago and Darin Louck to confirm the fact that the search and detention of Plaintiff's electronic devices on November 3, 2010, occurred at the functional equivalent of the border and thus constituted a border search. Those Declarations establish that Plaintiff remained in the O'Hare federal inspection services (FIS) area during the entire time he spoke with the ICE agents and when his electronic devices were detained. See Defs. 56.1 St., ¶¶ 2-6.

Reasonable suspicion may be required for non-routine *personal* searches, such as strip, body cavity, or involuntary x-ray searches. *See Flores-Montano*, 541 U.S. at 152; *Rahman v. Chertoff*, 530 F.3d 622, 624 (7th Cir. 2008) (holding only "[s]tops that entail intrusive searches of the body are in a special category"). Generally, the only searches that have been "held as nonroutine border searches are the ones that involve strip searches and body cavity searches." *United States v. Amaro-Rodriguez*, No. 08-378, 2010 WL 503063, at *2 (D.P.R. Feb. 8, 2010); *Barrow*, 448 F.3d at 41 ("Non-routine border searches include strip searches and body-cavity searches and can only be made if supported by a reasonable suspicion.").

Plaintiff does not allege that he was subject to any personally invasive searches, such as a strip search or body cavity search. Courts have upheld the warrantless searches of *objects* at the border without any level of suspicion, unless the search was conducted in a "particularly offensive manner" or resulted in excessive damage. *See Flores-Montano*, 541 U.S. at 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13).⁸ The November 3, 2010, search and inspection of Plaintiff's electronic devices fails to satisfy either of these standards.

C. Electronic Devices Are Closed Containers, and, as Such, Can Be Searched and Inspected at the Border Without Individualized Suspicion

Plaintiff was carrying various electronic devices (laptop, digital camera, flash drive, and cell phone) when he presented himself for inspection at O'Hare Airport on November 3, 2010.

Like a suitcase, purse, or duffel bag, Plaintiff's devices are subject to routine search and inspection at the border. As a result, the Government had the authority to inspect those devices, and to detain them for the time necessary to conduct a meaningful search in order to determine if

⁸ But even this standard has been held to permit some level of damaging force during a border search of an object. *See generally United States v. Chaudhry*, 424 F.3d 1051, 1054 (9th Cir. 2005); *United States v. Lawson*, 461 F.3d 697, 701-02 (6th Cir. 2006) (X-ray of luggage and "cut[ting] the liner in her luggage, then drill[ing] a hole in it" were permissible without individualized suspicion). Indeed, the border search upheld by the Supreme Court in *Flores-Montano* involved the "removal, disassembly, and reassembly of a fuel tank." *Flores-Montano*, 541 U.S. at 154 n.2.

the devices contained unlawful merchandise, or evidence of such merchandise, contraband, or criminal activity. In his Complaint, Plaintiff makes a variety of allegations about his electronic devices to essentially argue for an "electronic device" exception to the Government's border search authority. No such exception has ever been accepted by an authoritative federal court ruling, nor is one warranted.

Plaintiff alleges that his "computer and other electronic devices contained private and sensitive materials which he did not intend to expose to view by others without his consent."

Compl. ¶ 28. Of particular concern to Plaintiff is "information concerning his work on behalf of the [Bradley Manning] Support Network which [Plaintiff] chose to record or store in these devices," including "the complete Support Network mailing list, confidential communications between members of the Steering committee about strategy and fund-raising activities, the identit[ies] of donors, lists of potential donors and their ability to contribute, and notes on meetings with donors including personal observations about those donors." *Id.* ¶¶ 28, 30.

Information stored on Plaintiff's devices allegedly spans a period of years, including emails "sent to and from family members and friends and messages concerning employment related matters, records of his personal finances, computer programming work in progress, and passwords allowing access to his bank account, his workplace computer, and secure communications websites." *Id.* ¶ 29.

A large number of federal courts have already rejected Plaintiff's argument that the special nature of electronic devices requires an additional level of suspicion for searches at the border. These courts have recognized that electronic devices are similar to luggage and other closed containers and concluded that customs officers are entitled to inspect the contents of electronic devices without showing particularized suspicion. *See, e.g., United States v. Arnold,*

533 F.3d 1003, 1009 (9th Cir. 2008) (search of laptop, despite its sizeable storage capabilities, and personal nature, is no "different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed"); *United States v. Linarez-Delgado*, 259 Fed. Appx. 506, 508 (3d Cir. 2007) ("Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search."); *United States v. Ickes*, 393 F.3d 501, 504-05 (4th Cir. 2005) (holding defendant's computer and disks were "cargo" and thus subject to routine search and inspection at the border); *Cancel-Rios v. United States*, No. 10-1386, 2010 WL 3420805, at *3 (D.P.R. Aug. 30, 2010) (border search of cell phone did not require reasonable suspicion); *United States v. Hampe*, No. CR 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007) (Report and Recommendation holding that a search of computer at border "did not implicate any of the serious concerns that would justify characterizing this particular search as 'non-routine'"), *adopted*, 2007 WL 1806671 (D. Me. June 19, 2007).

None of Plaintiff's allegations provide a basis for this Court to depart from this long line of authority. Any personal information Plaintiff allegedly stored on these devices (Compl. ¶¶ 28-30) does not suffice to show that the inspection of his devices was a non-routine border search. *See United States v. Giberson*, 527 F.3d 882, 888 (9th Cir. 2008) (holding that "neither the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth

⁹

⁹ See also United States v. Veema, No. H-08-699-1, 2010 WL 1427261, *4 (S.D. Tex. Apr. 8, 2010) ("The search did not invade Verma's body or damage his computer. Therefore, the search at issue in the instant case is routine."); United States v. Bunty, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008) (border searches of laptops "do not require reasonable suspicion"); United States v. McAuley, 563 F. Supp. 2d 672, 677, 679 (W.D. Tx. 2008) ("Relying on the Supreme Court's reasoning in Flores-Montano, this Court cannot equate the search of a computer with the search of a person. The Court finds that the search of a computer is more analogous to the search of a vehicle and/or its contents." Also holding "that the search of one's personal computer at a port of entry is a routine search and thus, does not necessitate a finding of reasonable suspicion"); United States v. Pickett, No. 07-374, 2008 WL 4330247, *3-*4 (E.D. La. Sept. 16, 2008) ("search of his laptop and electronic devices was a non-invasive routine search that did not require reasonable suspicion"), aff'd, 598 F.3d 231 (5th Cir. 2010); United States v. Irving, No. 03-cr-633, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003) (search of camera and computer diskettes was a "routine border search"), aff'd, 452 F.3d 110 (2d Cir. 2006).

Amendment context"); *Arnold*, 533 F.3d at 1009 ("the Supreme Court has refused to draw distinctions between containers of information and contraband with respect to their quality or nature for purposes of determining the appropriate level of Fourth Amendment protection"); *see also Ickes*, 393 F.3d at 504-05 (noting Congress intended a "broad" definition of cargo and declining to carve out an exception for electronic devices simply because they contained "expressive" material).

Moreover, other containers can contain hard copies of the very same type of private information—including letters, diaries, photographs, love letters, day planners, names and addresses of associates, business and membership cards, client and donation lists, meeting notes, medical records, and personal reading materials. See McAuley, 563 F. Supp. 2d at 677-78 (refusing to "impute the same level of privacy and dignity afforded to the sovereignty of a person's being to an inanimate object like a computer," and recognizing that "[a] computer is simply an inanimate object made up of microprocessors and wires which happens to efficiently condense and digitize" written information, such as Social Security cards, medical records, and day planners, which are already subject to routine border searches). Plaintiff's allegations about the quality and nature of the information he chose to store on his electronic devices do not distinguish electronic devices from other closed containers. Luggage and other containers may also contain information related to the activities of groups or contain expressive materials, in written and other forms. See Church of Scientology of Cal. v. Simon, 460 F. Supp. 56, 57-58 (C.D. Cal. 1978) (three-judge panel rejected First Amendment challenge to seizure of "Church of Scientology's papers, which consisted of many thousands of pages); United States v. 12 200-Ft. Reels of Super 8mm Film, 413 U.S. 123, 125 (1973) (border search finding "movie films, color slides, photographs, and other printed and graphic materials"); United States v. Seljan, 547 F.3d

993, 1003 (9th Cir. 2008) (*en banc*) ("an envelope containing personal correspondence is not uniquely protected . . . at the border."), *cert. denied*, 129 S. Ct. 1368 (2009). Courts have specifically rejected claims that reasonable suspicion should be required for border searches of electronic devices because they may contain expressive material. *See Arnold*, 533 F.3d at 1010; *Ickes*, 393 F.3d at 507.

Moreover, there are good reasons *not* to create such an exception from the government's general border search authority for electronic devices. First, the level of suspicion required for border searches would then depend on the form in which the document is kept (hard copy or electronic). Not only would this mean that a traveler's privacy in their personal information would depend on whether the data is reproduced with ink and paper or stored in a computer, but it would also give safe haven to criminals of all types (and terrorists) who may cross U.S. borders knowing their plans and schemes are safely kept free from inspection on electronic devices. Second, carving out a special exception for information contained electronic devices would improperly favor certain travelers at the expense of others. Travelers who carry their information in computers would enjoy greater privacy protection than travelers who carry their information in hard copy form. For example, under Plaintiffs' approach, a sexually explicit and exploitative hard copy photograph of a child could be inspected without reasonable suspicion, but the very same photograph saved as an electronic file on a computer could be inspected only with reasonable suspicion.

The Fourth Amendment does not require a heightened level of protection for information based on how it is maintained or for persons who can store and transfer their records via electronic devices rather than through hard copies. *See United States v. Williams*, 592 F.3d 511, 523 (4th Cir. 2010) ("At bottom, we conclude that the sheer amount of information contained on

a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents."); *Giberson*, 527 F.3d at 888 ("Once again, Giberson's purported exception generates more questions than answers: If we permit a person's Day-Timer to be searched, what about one's BlackBerry? The format of a record or document should not be dispositive to a Fourth Amendment inquiry.").

Finally, devising complicated and layered rules for the searches of electronic devices at the border, based on the view that they are "special" is the kind of "complex balancing test" (Flores-Montano, 541 U.S. at 152) for evaluating the reasonableness of border stops that the Supreme Court has warned against and refused to embrace: "subtle verbal gradations" on the standard of reasonableness that "may obscure rather than elucidate . . ." Montoya de Hernandez, 473 U.S. at 541. Indeed, courts have noted that requiring reasonable suspicion for computer searches "effectively would allow individuals to render graphic contraband, such as child pornography, largely immune to border search simply by scanning images onto a computer disk before arriving at the border." Irving, 2003 WL 22127913, *5; accord Ickes, 393 F.3d at 506 (to "create a sanctuary at the border for all expressive material—even [] terrorist plans . . . would undermine the compelling reasons that lie at the very heart of the border search doctrine"). Under that view, smugglers and terrorists would have an obvious and overwhelming incentive to transfer their contraband, or evidence relating thereto, onto a computer before bringing contraband into the country. Courts have cautioned against imposing such "imprudent" constraints on federal officials. See Seljan, 547 F.3d at 1005 n.9 (rejecting argument that customs officials must have reasonable suspicion to search correspondence contained within Federal Express package; "such an imprudent constraint could have disastrous consequences: To avoid detection, a terrorist could simply enclose in a separate sealed envelope within the FedEx

package plans for an explosive device, instructions for an attack, the chemical formula for some form of poison, or any other type of document that could, under Seljan's proposed rule, qualify as unsearchable.").

However personal the information stored on electronic devices, or however vital it is to Plaintiff's daily life (Compl. ¶¶ 28-30), the same can be said for day planners, diaries, books, tax records, prescription medications, and any other item that a particular traveler might deem necessary for travel because it serves an important function. The Fourth Amendment was not intended to shield travelers from "inconvenience . . . at the international border." *Flores-Montano*, 541 U.S. at 155 n.3. As with all containers brought across the border, the traveler alone ultimately decides what content the electronic device will store and, more importantly, whether to bring that device, or all of the information stored on it, across the border at all.

D. Plaintiffs' Allegations that he was Targeted for the November 3, 2010 Search and Detention of his Electronic Devices Fail to State a Claim For Relief Under the Fourth Amendment

Plaintiff alleges that he was "targeted" for Government surveillance, such as the November 3, 2010 search and detention of his electronic devices, because "of [his] lawful and constitutionally-protected advocacy and associational activity" on behalf of the Manning Support Network. Compl. ¶ 14. Allegations about an officer's subjective motives for a border search are irrelevant for Fourth Amendment purposes. *See United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006). The Supreme Court has consistently rejected such claims, ruling instead that the central question is whether objective circumstances justified the search. *See, e.g., Whren v. United States*, 517 U.S. 806, 813 (1996) (stating that "we have been unwilling to entertain Fourth Amendment challenges based on the actual motivations of individual officers"); *United States v. Villamonte-Marquez*, 462 U.S. 579, 584 n. 3 (1983) (rejecting defendants' claim that suspicion-

free stop of shipping vessel was unlawful because "[c]ustoms officers were accompanied by a Louisiana State Policeman, and were following an informant's tip that a vessel in the ship channel was thought to be carrying marijuana" and were not looking to merely inspect the vessel's registration papers) (citing holding in *Scott v. United States*, 436 U.S. 128, 136-37 (1975) that under the Fourth Amendment, courts review "challenged searches under a standard of objective reasonableness without regard to the underlying intent or motivation of the officers involved."). The court in *Irving* explained that:

As pretext should not determine the validity of a border search, it also should not determine whether a border search is routine (meaning it does not require reasonable suspicion). Rather, as we have earlier held, the level of intrusion into a person's privacy is what determines whether a border search is routine. And, we have long ruled that searches of a person's luggage or personal belongings are routine searches.

452 F.3d at 124. As explained above, electronic devices are modern-day examples of "closed containers," like a suitcase or a purse; as a result, the search and detention of Plaintiffs electronic devices on November 3, 2010, was a reasonable and routine border search. Allegations that Plaintiff was singled out for this kind of routine search are irrelevant to his Fourth Amendment claim. *See Bond v. United States*, 529 U.S. 334, 339, n. 2 (2000) (applying *Whren* to determine if an officer's conduct amounted to a "search" under the Fourth Amendment because "the issue is not his state of mind, but the objective effect of his actions").

Moreover, even if such allegations were relevant, which they are not, nothing in the Complaint reasonably suggests that Plaintiff was "targeted" for a border search on November 3, 2010, as a result of his "lawful and constitutionally-protected advocacy and associational activity" on behalf of the Manning Support Network. Compl. ¶ 14. This conclusory allegation is based entirely on Plaintiff's surmise that he has been stopped several times while traveling and "questioned" about his "work with the Support Network or his political beliefs and activities."

Compl. ¶ 14. But Plaintiff's devices were detained on November 3, 2010, over nine months ago; the Complaint is devoid of any allegations of further government action against either Plaintiff or the Support Network. *See infra* at III. As a result, there are no plausible allegations of any effort by the Government to target Plaintiff or the Support Network through the November 3, 2010 border search. *See Iqbal*, 129 S. Ct. at 1949 ("naked assertion[s]" of wrongdoing fall short of the plausible allegations required to withstand a motion to dismiss).

E. Detaining Devices is Consistent With the Government's Need to Adequately Inspect Items Before They Enter the United States

Plaintiff also contends that the "prolonged detention" of his electronic devices served to violate the Fourth Amendment. Compl. ¶ 37. As noted in the Complaint, Plaintiff's devices were detained on November 3, 2010, and they were returned to him on December 22, 2010, forty-nine days later. According to Plaintiff, this was simply too long a time for the Government to have detained his devices. This allegation fails to state a claim for relief because the Fourth Amendment does not set any rigid limit on the permissible duration of a border search. Indeed, "the Supreme Court has 'consistently rejected hard-and-fast time limits' in evaluating the reasonableness of border searches and has stressed that 'common sense and ordinary human experience must govern over rigid criteria." *Tabbaa v. Chertoff*, 509 F.3d 89, 100 (2d Cir. 2007) (quoting *Montoya de Hernandez*, 473 U.S. at 543). The Ninth Circuit recently reiterated that the "border search doctrine is flexible enough to meet the evolving demands inherent in securing our nation's borders." *Cotterman*, 637 F.3d at 1083.

The reality is that with electronic devices adequate inspections may take more time, not less. During the inspection, the devices and/or information have *not* yet been cleared for entry into the United States; the Government has only retained custody of the material until it can conduct an adequate inspection. *See Cotterman*, 673 F.3d at 1077. To accommodate the traveler

to the greatest extent possible, while fulfilling the Government's obligation to secure the border, ICE policy allows, in appropriate cases, the return of the devices to the traveler while the border search continues on the copies of the information contained therein. ICE Directive, \$8.1(5). In this way, ICE is able to minimize, to the extent possible, the effect of the border search on the traveler because the amount of time for an inspection of an electronic device varies.

Courts have acknowledged that the process of searching files in a computer or other electronic device "can take a long time" since, as even Plaintiff acknowledges in his Complaint, ¶¶ 28-29, his devices may contain many files. See, e.g., United States v. Burgess, 576 F.3d 1078, 1092–94 (10th Cir. 2009) ("[T]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files."). ¹¹ Reviewing such a large amount of information, to thoroughly inspect for contraband or other unlawful merchandise, takes time. See United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("Images can be hidden in all manner of files, even word processing documents and spreadsheets . . . There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it."). Adequate inspection may also require transporting the devices to another location, where additional review can take place. See Cotterman, 637 F.3d at 1078 (noting that the "complexity of some property, specifically computer equipment, often will require the Government to seize that property and relocate it to a secondary site in order to adequately conduct a meaningful search").

-

¹⁰ The alternative would be to detain the original for the entire search, thus depriving the individual of the use of their electronic media for a longer period.

The cases cited involve computers searched pursuant to a warrant, but the language regarding the time it can take to search a computer is just as applicable to border searches. *See also United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 48 (D. Conn. 2002) (searching a seized computer "could takes weeks or months"); *United States v. Mitchell*, No. CR407-126, 2007 WL 2915889, *11 (S.D. Ga. Oct 3, 2007) (Report and Recommendation) (search of computer "often takes considerable time . . . to analyze a storage device containing many gigabytes of data"), *adopted*, 2007 WL 3102167 (S.D. Ga. Oct. 22, 2007).

Accepting an individual's word for what is located on his or her electronic devices, or even assuming that computer files are what their filenames suggest, would do little to advance the Government's interest in preventing the entry of contraband or unlawful merchandise. *See United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006) (government should not be required to trust an individual's self-labeling because "computer files are easy to disguise or rename"); *United States v. Stabile*, 633 F.3d 219, 237 (10th Cir. 2011) (noting that "criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required"). Searches of electronic devices also pose special difficulties because there is a risk that officers might damage or compromise a file by attempting to access the data. *Hill*, 459 F.3d at 974 (quoting *United States v. Hill*, 322 F. Supp. 2d 1081, 1089 (C.D. Cal. 2004)). Because of this, experts often make a back-up copy of the contents before beginning their search. *Id.* Simply put, examining a computer is complicated and time-consuming.

None of this offends the Fourth Amendment because without adequate time and resources, the electronic devices cannot be adequately inspected, and the Government cannot fully discharge its obligation to faithfully secure our borders. In the end, the Government has the authority to search and detain items (including electronic devices) at the border, and it is permitted to detain those items for a sufficient time in order to conduct an adequate inspection. Plaintiff's Fourth Amendment claim regarding the "prolonged" detention of his devices should therefore be dismissed.

F. In the Alternative, Even if the Court Finds that Plaintiff has Stated a
Claim for a Fourth Amendment Violation, the Undisputed Material Facts
Show that the Detention of Plaintiff's Devices was Reasonable, and the
Court Should Award Summary Judgment to the Government on this Claim

The Government's detention of Plaintiff's electronic devices between November 3, 2010 and December 17, 2010 was reasonable, because Plaintiff's items had not been cleared for entry into the United States, and remained in the control of the Government, so that the Government could still continue the border search. During this time, ICE continued its inspection of the detained devices. ICE Directive, ¶ 8.3(1). In fact, Plaintiff first inquired about the return of his devices at the same time they had already been shipped to him. *See* Compl. ¶ 21; Defs. 56.1 St. ¶¶ 7-8.

Defendants' Rule 56.1 Statement establishes that Plaintiff's devices were held no longer than necessary. During the time Plaintiff's devices were detained by ICE, "images of the detained media were forensically prepared and reviewed by a properly trained ICE Computer Forensic Agent." Defs. 56.1 St. ¶ 9. This process "was to ensure that the imaged data was intact and accessible for review." Defs. 56.1 St. ¶ 10. ICE policy provides that searches of electronic devices are generally to be completed within thirty calendar days of the date of the detention, unless circumstances exist that warrant more time. ICE Directive ¶ 8.3(1). Plaintiff's devices were retained in excess of 30 days, for several reasons. First, Plaintiff declined to provide any access passwords to his digital media as required by law, *see* 19 U.S.C. § 507; 19 C.F.R. §148.21. Defs. 56.1 St. ¶ 12. The lack of a password required ICE agents to spend additional time reviewing Plaintiff's devices. Defs. 56.1 St. ¶ 13. Second, Plaintiff's laptop featured a non-standard configuration and utilization of software, including an operating system (Linux), with which the ICE agents were less familiar. Defs. 56.1 St. ¶¶ 14-15. Third, to check that the images of Plaintiff's devices had been made correctly, a separate computer had to be set up with

forensic software. Defs. 56.1 St. ¶ 16. Finally, there are a limited number of ICE agents who are certified in computer forensics; these agents are responsible for a multitude of activities, including border searches at approximately 327 different ports of entry, as well as computer searches resulting from consent or the issuance of warrants in cases assigned to over 7,000 ICE Special Agents. Defs. 56.1 St. ¶¶ 17-18. 12

The fact that Plaintiff thinks five weeks was an overly long period of time for his devices to be detained by ICE fails to state a claim for relief under the Fourth Amendment. The question is whether the detention remained "reasonably related in scope to the circumstances which justified it initially." *Montoya de Hernandez*, 473 U.S. at 542; *see also Illinois v. Caballes*, 543 U.S. 405, 407 (2005). To make this determination, the Court is obliged not to "indulge in 'unrealistic second-guessing. . . .'" *Montoya de Hernandez*, 473 U.S. at 542 (quoting *U.S. v. Sharpe*, 470 U.S. 675, 686 (1985)). The undisputed material facts show that ICE acted reasonably in detaining Plaintiff's devices.

III. PLAINTIFF'S FIRST AMENDMENT CLAIMS SHOULD BE DISMISSED

Plaintiff's First Amendment claim derives from his contention that the Government should not be able to search and detain his electronic devices without reasonable suspicion because the devices contain personal information. An otherwise valid search under the Fourth Amendment does not violate the First Amendment rights of an individual simply because the search uncovers expressive materials. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 563-68 (1978). This premise is equally applicable in the border search context. In *United States v. Borello*, 766 F.2d 46 (2d Cir. 1985), the Second Circuit recognized that the search and seizure of

The copies of Plaintiff's devices are now being retained only for the purposes of litigation. *See* Defs. 56.1 St. \P 20.

In response to *Zurcher*, Congress enacted the Privacy Protection Act, which generally prohibits the search or seizure of "any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. § 2000aa(a). Congress explicitly exempted customs and border searches from this prohibition. *See* 42 U.S.C. § 2000aa-5.

films that were "not legally obscene" in the course of a "reasonable border search" did not implicate the First Amendment. *Id.* at 58 ("Surely, Customs officials can permissibly screen [expressive] materials entering the country to enforce [criminal] laws."). *See also Church of Scientology of Cal.*, 460 F. Supp. at 59 (border search "necessarily involves the examination or review of [written materials], for the customs officers must scan or peruse and perhaps even read the material to determine whether or not they are importable"). Reasonable suspicion is not required for a routine border search of material, "expressive" or not.

A. The November 3, 2010 Search and Inspection of Plaintiff's Devices Did not Violate his First Amendment Rights

Plaintiff's claim that Defendants violated his First Amendment rights during the November 3, 2010 search and inspection of his electronic devices repeats his argument that personal electronic devices should not be subject to border searches. As stated above, there is no basis to apply a different rule to the search of electronic devices at the border. Indeed, both the Fourth and Ninth Circuits have squarely rejected attempts "to carve out a First Amendment exception to the border search doctrine" in the context of laptop searches. *See Ickes*, 393 F.3d at 506; *Arnold*, 533 F.3d at 1010. As these courts observed, such an exception would:

(1) protect terrorist communications "which are inherently 'expressive'; (2) create an unworkable standard for government agents who "would have to decide — on their feet — which expressive material is covered by the First Amendment"; and (3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First Amendment interest is also at stake.

Arnold, 533 F.3d at 1010 (quoting *Ickes*, 393 F.3d at 506-08). Plaintiff's First Amendment challenge to the November 3, 2010 search must be rejected for the same reasons. The fact that his electronic devices contained expressive material does not make the search invalid. Customs

officials have the right to look at expressive materials, whether they are included on electronic devices or on paper, film, or other mediums. *See Borello*, 766 F.2d at 58; *Ickes*, 393 F.3d at 506; *Arnold*, 533 F.3d at 1010.

B. Plaintiff's Associational Privacy Claim Should Be Dismissed

Plaintiff also asserts a claim for violations of his "right of associational privacy" because the detention of his devices by the Government presents a threat to the "organization, work, and supporters and donors of the Bradley Manning Support Network" (Compl. ¶ 38)—in violation of the First Amendment. Plaintiff predicts that the Government's retention or disclosure of this information will "materially interfere with lawful activities and association in support of Manning's defense" because "some supporters and contributors to the Support Network will contribute to the Manning defense or otherwise support the work of the Support Network only if their support can remain anonymous." Compl. ¶¶ 35, 38. This claim should be dismissed because there is no factual context supporting these conclusory allegations, as required by *Iqbal*, 129 S. Ct. at 1954. As an initial matter, Plaintiff's right to associate with others for expressive purposes is not absolute. See Roberts v. United States Jaycees, 468 U.S. 609, 622-23 (1984). Mere incidental burdens on the right to associate do not violate the First Amendment; rather, the interference with Plaintiff's associational rights must be "direct and substantial" or "significant." Lyng v. Int'l Union, 485 U.S. 360, 366-67, 379 & n. 5 (1988). Instead, "the First Amendment privilege generally guarantees the right to maintain private associations when, without that privacy, there is a chance that there may be no association and, consequently, no expression of the ideas that association helps to foster." In Re Motor Fuel Temperature Sales Practices Litig., 641 F.3d 470, 479 (10th Cir. 2011).

Here, any alleged infringement on Plaintiff's "right of association" was incidental to a valid exercise of the Government's authority to search and detain personal items at the border. Plaintiff is not free from search and inspection at the border simply because he is a member of a group.

While the Complaint generally avers that "Plaintiffs and other individuals who have publicly supported Mr. Manning" (Compl. ¶ 34) have been identified by name and targeted, the Complaint is devoid of any additional details about how Support Network members have been "targeted" by the Government. Statements about the "highly charged and politically controversial" nature of the Manning prosecution (Compl. ¶ 34) do not plausibly demonstrate an effort by the Government to pursue the Support Network.¹⁴ In addition, while Plaintiff speculates that the detention of his devices will "materially interfere with lawful activities and association in support of Manning's defense," (Compl. ¶ 35) there are no allegations of such interference, nor is there any basis for the Court to presume such an outcome is imminent or even likely. Plaintiff's speculation—unsupported by any substantive allegations—about what he thinks may happen does not suffice. While Plaintiff contends that he has been "visited and questioned, both at his home and place of work in Cambridge, by investigators for the U.S. Department of Defense, the Department of State, and the Federal Bureau of Investigation," (Compl. ¶¶ 14, 35), this does not make out a claim for infringement on his right to association. There is also no right to be free from questioning by Government personnel simply because one is a member of a group.¹⁵

To the extent that Plaintiff and others may have been identified by name, this identification cannot be surprising since their support for Mr. Manning has concededly been "public." Compl. ¶ 34.

¹⁵ In addition, these entities are not Defendants in this matter, and Plaintiff's complaint makes no effort to connect the alleged questioning by these other federal agencies to the November 3, 2010 search and detention of his electronic devices.

Ultimately, the particular search at issue involved only Plaintiff (not other members of the Support Network), and the Complaint lacks any allegations of follow-up activity by the Government against either Plaintiff, the Support Network, or other Support Network members in the 260-plus days that have elapsed since Plaintiff's electronic devices were detained. Such allegations are required to make out a claim for a violation of associational privacy. See Motor Fuel Temperature Sales, 641 F.3d at 489 (explaining that First Amendment privilege from compelled disclosure "generally ensures privacy in association when exposure of that association will make it less likely that association will occur in the future, or when exposure will make it more difficult for members of an association to foster their beliefs."). There is no basis to support Plaintiff's prediction about the likelihood of eroding participation in the Support Network as a result of the detention of his personal electronic devices. Plaintiff's entire supposition appears to rest on his generalized statement that the Manning prosecution is "highly charged and politically controversial." Compl. ¶ 34. This fails to show the kind of concrete "harassment and intimidation" courts have required of parties claiming a First Amendment chilling effect. Motor Fuel Temperature Sales Practices Litig., 641 F.3d at 491; see also Doyle v. N.Y. State Div. of Hous. and Cm'ty Renewal, No. 98- 2161, 1999 WL 177441, at *7 (S.D.N.Y. Mar. 30, 1999) (ruling plaintiffs failed to show "a history of retaliation nor even a commonsense practical likelihood of retaliation from the disclosure of membership in the [Stuyvesant Town-Peter Cooper Village Tenants Association or from disclosure of opposition to rent increases").

In contrast, in *Tabbaa v. Chertoff*, 509 F.3d 89, 102-03 (2d Cir. 2007), the Second Circuit concluded that a series of border stops of individuals who had all attended a conference in Canada did constitute a burden on the individuals' right of association, because the individuals were "detained for a lengthy period of time, interrogated, fingerprinted, and photographed" and

the Court concluded that "the prospect of being singled out for such extensive processing could reasonably deter others from associating at similar conferences." *Id.* at 102. Despite this burden, the court ultimately concluded that the searches and detentions of the *Tabbaa* plaintiffs were justified by the government's compelling interest in "protecting the nation from terrorism." *Id.* at 103.

There is nothing in Plaintiff's Complaint that alleges or even reasonably suggests that the Government has used its border search authority to expose the members and operations of the Support Network. This is in contrast to cases in which courts found the compelled disclosure of an association's members to be a First Amendment violation, based on facts indicating the group was specifically singled out. In Brown v. Socialist Workers '74 Campaign Comm. (Ohio), 459 U.S. 87, 101-02 (1982), the Supreme Court invalidated the application of a law requiring disclosure of membership lists for the Socialist Workers Party (SWP), in part because there was past 15-year history of "massive" Government harassment of the party, "suggest[ing] that hostility toward the SWP is ingrained, and likely to continue." See also NAACP v. Alabama ex rel. Patterson, 357 U. S. 449, 462 (1958) (compulsory disclosure of the membership lists of an organization, which led to harassment, physical threats, and economic reprisals against those individuals, worked "a substantial restraint upon the exercise by petitioner's members of their right to freedom of association"). Here, Plaintiff's own complaint states that ICE and CBP released policies addressing the search and detention of electronic devices in 2009 (Compl. ¶¶ 24-26)—over a year before his devices were even detained upon his return from Mexico, and in all that time, Plaintiff has not alleged any other instances of suspected retaliation or harassment by the Government.

CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court grant their

Motion to Dismiss, or in the Alternative, for Summary Judgment.

Dated: July 28, 2011 Respectfully submitted,

TONY WEST

Assistant Attorney General

CARMEN M. ORTIZ United States Attorney

BARBARA HEALY SMITH Assistant U.S. Attorney

SANDRA M. SCHRAIBMAN Assistant Branch Director

s/Diane Kelleher

DIANE KELLEHER

Senior Trial Counsel

U.S. Department of Justice, Civil Division

Federal Programs Branch

20 Massachusetts Ave., N.W., Room 7318

Washington, D.C. 20530 Tel.: (202) 514-4775 Fax.: (202) 616-8470

Email: diane.kelleher@usdoj.gov

CERTIFICATION OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non registered participants by First Class Mail, on the 28th of July, 2011.

/s/Diane Kelleher DIANE KELLEHER July 28, 2011